PATENT
P55690

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Chang-Hyi LEE

Serial No.:   09/302,431

Filed: 30 April 1999

For: COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

Examiner: B. E. Lanier

Art Unit: 2132

Appeal No._____

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

    ATTENTION: Board of Patent Appeals and Interferences

    <u>**APPELLANT'S BRIEF (37 CFR §1.192)**</u>

    This brief is in furtherance of the Notice of Appeal filed in this case on 2 June 2004.

    The fees required under §1.17(f) for the filing of the Appellant's Brief are dealt with in the accompanying transmittal letter.

    This brief is transmitted in triplicate (37 CFR §1.192(a)).

Folio: P55690
Date: 7/26/04
I.D.: REB/MDP

APPEAL BRIEF

I.   STATEMENT OF REAL PARTY IN INTEREST

Pursuant to 37 CFR §1.192(c)(1) the real party in interest is:

> SamSung Electronics Co., Ltd.
> 416 Maetan-dong, Yeongtong-gu,
> Suwon-si, Gyeonggi-do,
> Republic of Korea

II.   RELATED APPEALS AND INTERFERENCES

Pursuant to 37 CFR §1.192(c)(2), there are no appeals nor interferences known to the Appellant, the Appellant's legal representative, or the Assignee (real party of interest) which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III.   STATUS OF CLAIMS

Claims 1-3, 5-7 and 9-40 stand rejected. Accordingly, the rejection of claims 1-3, 5-7 and 9-40 is appealed herein.

IV.   STATUS OF AMENDMENTS AFTER FINAL REJECTION

The Advisory Action (Paper No. 22) fails to indicate whether or not the Amendment filed 23 April 2004 was entered. Since the only amendment was to correct a misspelled word, we will assume that the Amendment has been entered.

V.   SUMMARY OF THE INVENTION

CA stands for Certificate Authority (e.g., secure digital music initiative (SDMI), or other trust third party).

LCM stands for Licensed SDMI Compliant Module.

PD stands for SDMI Compliant Portable Device.

PDFM stands for Portable Device Functional Module.

ISP stands for Internet Service Provider (including Content Provider via the Internet).

PM stands for Portable Media (SDMI Compliant Storage Media).

Furthermore, here are presented some notations to be used in the following sections. Even though they are some intricate, we are sure that they would help the readers clearly understand the concrete method we intend. They are relevant to the algorithmic functional modules.

ECC - Elliptic Curve Cryptosystem

$PryKey_A$, $PubKey_A$ - Private Key and Public Key of A (this may be LCM, PD (optional), ISP, CA,...), respectively.

$Cert_{CA}$ ($PubKey_A$) - A Certificate for a Public Key $PubKey_A$ issued by CA.

MK_{PD} - The Manufacturer Key within a PD

ID_{MK} - The Indicator of a Manufacturer Key.

CK_{PD-LCM} - This is a secure (secret) channel key which is setup between PD and LCM.

EC_ENC(*key, C*) - Elliptic Curve based Encryption of a content *C* by utilizing a public key, *key*.

EC_DEC(*key, C*) - Elliptic Curve based Decryption of a ciphertext (encrypted text) *C* by utilizing a private key, *key*.

EC_DH(*A,B)* - A random secret value (key) shared between *A* and *B* by Elliptic Curve based

Diffie-Hellman Key Exchanging Protocol.

ENC(*key, C*) - Symmetric Key Encryption of a content C by utilizing a secret key, *key*;

(DEC(*key,C*) - Symmetric key decryption of a ciphertext C by utilizing a secret key, *key*;

AIF - Algorithm Identifying Field

API - Applied Program Interface

CCS - Copy Control Status

CDF - Content Description Field

CEK - Content Encryption Key

CertCA (PubKeyA) - Certificate (Data) for PubKeyA issued by CA

CHI - Copyright Holder Information Field

CTC - Copyright, Transfer, Check-in/Check-out

ECC - Elliptic Curve based Cryptosystem

EC_DH(ISP,LCM) - random secret value (key) shared between ISP and LCM by Elliptic

Curve (Cryptosystem) based Diffie-Hellman Key Exchanging Protocol

EC-ENC - Elliptic Curve-based Encryption of a content by utilizing a public key

ENC - Symmetric Key Encryption of a content by utilizing a secret key

ICL - Import Control Layer

ID_A - Identifier of A

IP - Information Provider;

ISP - Internet Service Provider including Content Provider via the network

LCM - Licensed SDMI Compliant Module

MKIT - Manufacturer Key Information Table

Page 4 of 57

MKPD - Manufacturer Key within a portable device

PCS - Playback Control Status

PD - SDMI Compliant Portable Device

PDFM - Portable Device Functional Module

PKC - Public Key Cryptosystem

PM - Portable Media (SDMI Complaint Storage Media)

PryKeyA, PubKeyA - Private Key and Public Key of A (A may be LCM, PD, ISP, CA, and

the like)

RMF - Right Management Field

RMS-DB - Right Management System-Data Base

RNG - Random Number Generation Unit

SDMI - Secure Digital Music Initiative

SH - Secret Header

SNAKE - Symmetric Key Encryption Algorithm, which is very effective for both software

and hardware implements and has been world-wide cryptanalized

SOI - Source Originator Indicator Field;

UTD - Update Token Data.

FIG. 1

A certificate authority 110 generates a first table having the manufacturer key and the

manufacturer key data, and a second table having an identifier (ID) of the portable device 150, a

token, T, and the information ($ENC(MK_{PD}, T)$) of the token encrypted by the manufacturing key.

That is, the certificate authority 110 generates the manufacturer key, MK_{PD}, and its certificate data, $Cert(MK_{PD})$, in accordance with a first registration request signal 121 inputted from a manufacturer 120 of portable devices 150, and outputs a manufacturer key and a manufacturer key data to the manufacturer 120.

The manufacturer 120 of the portable devices 150 outputs the registration request signal 121 to the certificate authority 110 and receives the manufacturer key and the manufacturer key data generated by certificate authority 110 in accordance with the first registration request signal 121.

An internet service provider (ISP) 130 including a content provider via the internet outputs a request signal 131 to the certificate authority 110, receives a pair of keys and the certificate of the key which are generated in the certificate authority 110 in response to the registration request signal 131 of the ISP, and the second table from the certificate authority 110.

A licensed SDMI (secure digital music initiative) compliant module (LCM) 140 as a first content output unit outputs a registration request signal 141 to the internet service provider 130 in order to receive the digital contents, receives the public key and the data of the public key generated in response to the request signal 141, bypasses the data of the manufacturing key of the portable device 150 to the ISP 130, and encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data.

The portable device 150 as a second content output unit stores the manufacturer key and the manufacturer key data transferred from the certificate authority 110, outputs its manufacturer key to the internet service provider 130 through the LCM 140, and receives the manufacturer key data of the second table, which is encrypted, supplied from the LCM in order to judge if the stored manufacturer key is authenticated.

FIG. 2

FIG. 2, contains the manufacturer key data (Cert(MK_{PD})), the manufacturer key (MK_{PD}), and an identifier (ID_{MK}) corresponding to the manufacturer key data and the manufacturer key, and is stored in only the certificate authority 110. Further, the second table is generated from the certificate authority 110 and outputted to the internet service provider 130, and contains the identifier(ID_{MK}), data ($ENC(MK_{PD}, T)$), and a token(T) which is encoded by the manufacturing key.

At this time, the certificate authority 110 forms a first channel key(k) which can be shared with the internet service provider 130 in accordance with the registration request signal 131 inputted from the internet service provider 130, and outputs the first authentication qualification key and the first authentication qualification key data 111 which are encoded into the internet service provider 130 through a secret channel formed by the first channel key(k).

The first channel key is a key generated from encryption of the certificate authority 110 by using the data which the internet service provider 130 has.

There are four registration mechanisms relative to ISPs, LCMs, and PDs. The four registration mechanisms include the registrations of the portable device manufacturers to the certificate authority, of ISP to the certificate authority, of LCM to ISP and of the portable device to LCM, and of multiple LCMs or multiple PDs. The manufacturers' registration to CA precedes ahead all the others.

The registration of the portable device manufacturer 120 to the certificate authority 110 is illustrated in FIG. 2.

When the manufacturer 120 requests its registration to CA 110, CA 110 certifies it and then generates a manufacturer key, MK_{PD}, and make its certificate data, $Cert_{CA}(MK_{PD})$, to deliver them to

the manufacturer 120. At the same time CA 110 generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for an ISP-registration. Once after the manufacturer 120 gets the data, $\{MK_{PD}, Cert_{CA}(MK_{PD})\}$, the manufacturer 120 can manufacture the portable devices by imbedding those secret data within a temper resistant area of the portable devices.

Therefore, the portable devices 150 manufactured by the manufacturer 120 are authorized by the certificate authority 110 to store the downloaded, encrypted digital contents.

Fig. 3

Fig. 3 shows how for the ISP 130 to register to CA 110 and what information to get from CA 110. For an ISP to register to CA, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between CA and itself by EC_DH(CA, ISP) and provide a safe way to communicate each other without allowing an illegal copy of the downloaded information through the channel. A pair of keys and key data $\{ PrvKey_{isp}, PubKey_{isp}, Cert_{CA}(PubKey_{ISP}) \}$ are generated and stored in the certificate authority 110, and two tables are formed in dependence with the manufacture key. The certificate authority 110 encrypts and transmits the encrypted key and key data to internet service provider 130 through the channel in order to co-own the key and key data. Secondly the ISP 130 gets its semi-permanent private-public key pair $\{PrvKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ and the manufacturer key information table data through the secure channel. Where CA''s certification to the ISP should be proceded ahead all these procedures. ISP's key pair should be securely stored.

The LCM''s key pair should be securely stored, where the host's various system parameters

may be used for this goal.

Here the LCM registration mechanism to an ISP together with PD registration is described. As in Fig. 4, LCM gets the ISP's Public Key Information $\{PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ at first and verifies its validity by using the CA's public key Information which was already announced or preset within the LCM in a code-imbedded-like method.

If the validity of the certificate for the ISP's public key is certified, the LCM 140 executes the handshaking protocol to get an ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel, the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP. When a request signal 151 is transmitted from the potable device 150 to the LCM 140, the portable device 150 tosses the certificate data for its ID of the manufacturer key to the LCM 140. The LCM 140 sends them to its connected ISP 130 in the encrypted form, $EC\_ENC(PubKey_{ISP,} Cert_{CA}(ID_{MK}))$.

The internet service provider 130 decrypts the encrypted information and compares the decrypted information with the information of the second table. If the decrypted information is identical to the information of the second table, the internet service provider 130 encrypts the content of the table and transmits it to the LCM 140 in a secure manner. The LCM 140 decrypts the encrypted information to obtain the information of the token. For the LCM 140 and the portable device 150 to set up a shared secret key and to complete the portable device registration, the LCM 140 randomly generates their static and secret channel key, CK_{PD-LCM}, and encrypts and sends $ENC(T,CK_{PD-LCM})\|T^*$. Upon receiving these data, the portable device 140 can extract the token value T from T^* by using the manufacturer key and, by using this token, the portable device 140 can also

compute CK_{PD-LCM} and store it. As the portable device 140 securely stores this channel key, the portable device registration is finished.

The channel key, CK_{PD-LCM}, may be originated from portable device 150 instead of LCM 140. In this case the portable device 150 receives the data T^* from the LCM and gets the token T by decrypting T^* with its manufacturer key. And then the portable device generates a random channel key CK_{PD-LCM} to upload $ENC(T, CK_{PD-LCM})$ to LCM.

The part of the record in the manufacturer key information table (MKIT) of the LCM 140 stays in encrypted form by using the LCM's secret key (this key may be LCM's public key).

In practice, during the portable device 150 registration to LCM 140,, an update token data (UTD) of Right Management System-Data Base (RMS-DB) should be transferred from the portable device 150 to the LCM 140 (or from the LCM 140 to the portable device 150) together with CK_{PD-LCM} and be set both in the RMS-DB and in the portable device. Therefore, all the units and terminals in this system are authorized to transmit and receive the encrypted digital contents between the units and terminals.

As shown in FIG. 1, the architecture and the file format of the present invention can allow users to register their own limited number of LCMs or PDs. The number may be limited by ISP or by CA.

To register a plurality of LCMs, since ISP maintains the private-public key pair of the firstly registered LCM of a user's multiple LCM's, ISP can securely deliver the same key pair to the another LCM of the user''s.

To register a plurality of portable devices, since LCM securely maintains the secret channel key between the LCM and PD, the LCM can securely deliver the same key pair to the another

portable device of the user's in the same manner depicted in Fig.4.

Fig. 4

Here the LCM registration mechanism to an ISP together with PD registration is described. As in Fig. 4, LCM gets the ISP's Public Key Information $\{PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ at first and verifies its validity by using the CA's public key Information which was already announced or preset within the LCM in a code-imbedded-like method.

If the validity of the certificate for the ISP's public key is certified, the LCM 140 executes the handshaking protocol to get an ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel, the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP. When a request signal 151 is transmitted from the potable device 150 to the LCM 140, the portable device 150 tosses the certificate data for its ID of the manufacturer key to the LCM 140. The LCM 140 sends them to its connected ISP 130 in the encrypted form, $EC\_ENC(PubKey_{ISP,} Cert_{CA}(ID_{MK}))$.

The internet service provider 130 decrypts the encrypted information and compares the decrypted information with the information of the second table. If the decrypted information is identical to the information of the second table, the internet service provider 130 encrypts the content of the table and transmits it to the LCM 140 in a secure manner. The LCM 140 decrypts the encrypted information to obtain the information of the token. For the LCM 140 and the portable device 150 to set up a shared secret key and to complete the portable device registration, the LCM 140 randomly generates their static and secret channel key, CK_{PD-LCM}, and encrypts and sends

ENC(T,CK_{PD-LCM})||T*. Upon receiving these data, the portable device 140 can extract the token value T from T* by using the manufacturer key and, by using this token, the portable device 140 can also compute CK_{PD-LCM} and store it. As the portable device 140 securely stores this channel key, the portable device registration is finished.

The channel key, CK_{PD-LCM}, may be originated from portable device 150 instead of LCM 140. In this case the portable device 150 receives the data T* from the LCM and gets the token T by decrypting T* with its manufacturer key. And then the portable device generates a random channel key CK_{PD-LCM} to upload ENC(T, CK_{PD-LCM}) to LCM.

The part of the record in the manufacturer key information table (MKIT) of the LCM 140 stays in encrypted form by using the LCM's secret key (this key may be LCM's public key).

In practice, during the portable device 150 registration to LCM 140,, an update token data (UTD) of Right Management System-Data Base (RMS-DB) should be transferred from the portable device 150 to the LCM 140 (or from the LCM 140 to the portable device 150) together with CK_{PD-LCM} and be set both in the RMS-DB and in the portable device. Therefore, all the units and terminals in this system are authorized to transmit and receive the encrypted digital contents between the units and terminals.

As shown in FIG. 1, the architecture and the file format of the present invention can allow users to register their own limited number of LCMs or PDs. The number may be limited by ISP or by CA.

To register a plurality of LCMs, since ISP maintains the private-public key pair of the firstly registered LCM of a user's multiple LCM's, ISP can securely deliver the same key pair to the another LCM of the user''s.

To register a plurality of portable devices, since LCM securely maintains the secret channel key between the LCM and PD, the LCM can securely deliver the same key pair to the another portable device of the user's in the same manner depicted in Fig.4.

Fig. 5

Fig. 5 shows exemplified implementation for the management rule of RMS-DB when a content downloading occurs.

To manage the information CTC={Copyright, Transfer, Check-in/Check-out}, the LCM140 maintains the Right Management System Database 143, named RMS-DB in a secure manner. The Right Management System is described, focusing on the content transaction between LCM 140 and PC 150.

The RMS-DB contains an update token data area 143a, a title, CTC (copyright, transfer, check-in/check-out) field 143b, a playback control status data area 143c (PCS: the permitted times to play, the amnesty period,...).

The part of the record in RMS-DB (in LCM) stays in encrypted form by using the LCM's secret key such as CK_{PD-LCM}.

The UTD part 143a may have a few number of Updating Token Data depending on the number of a user's own PDs.

The most important area in the database is the update token area 143a, and the update token area 143a has different values when the update token area 143a downloads a digital content from the LCM 140 to the portable device 150, or uploads the digital content from the portable device 150 to

the LCM 140. At this time, the update token is transmitted to the LCM 140 through the portable device 150 to update the stored token in the LCM 140.

A portable device import control is a layer existing in the LCM 140 to import SDMI Compliant contents from ISPs or to import non-SDMI Compliant outsource contents (e.g. RedBook CD, DVD,...). Therefore, this layer should contain such capabilities as the followings:

Trans-Coding to make PD decompress the input with its CODEC,

Trans-Encrypting to make PD decrypt the input with its Encryption System, and

Converting the input to SDMI Compliant the format.

PD Interface has the following capabilities:

Authenticating to PD, and

opening a secure channel between LCM and PD.

ISP Interface has the following capabilities:

Authenticating to PD, and

opening a secure channel between LCM and PD.

Functional Components in PDFM has LCM Interface and Import Control within PDFM.

LCM Interface has the following capabilities:

Authenticating to LCM, and

opening a secure channel between PD and LCM.

The import control within the portable device has the capability to import a outsource analog input and to make it fit to the SDMI Compliant file format. Where the converted SDMI Compliant content should have the binding information to the PD to be played only via the PD.

FIG. 6

FIG. 6 shows an exemplified file format.

As shown in FIG. 6, the SDMI compliant file contains a plain header 610, a secret header 620, and a file body 630. The plain header 610 comprises a title-ID 611, a content description field (CDF) 612 (e.g., Title, Composer, Artist, Record-label), and an algorithm identifying field (AIF) 613. The secret header 620 contains a device-identifier 621 (i.e., LCM_ID, PD_ID, or PM_ID), a source originator indicator field (SOI) 622 (i.e., ISP, LCM (CD-ripping, Audio input), PD (Analog input), or Kiosk), a copyright holder information field (CHI) 623, a right management field (RMF) 624, and a content encryption key 625. The file body 630 contains a symmetric key encryption of content by utilizing a secret key (ENC(k, Content)).

Right management field 624 contains the Copy (e.g., Copy-Never/Copy-Free/No-More-Copy mode), Check-In/Out mode, Transfer mode (i.e., transferable or not) and Playback Control Status (e.g., allowable number of times to be played (unlimited or n-times), expiration date, and amnesty period), which are to be encrypted by secret key of the device.

The rules to transfer contents securely over ISP-LCM-PD-PM are as follows.

When the ISP receives a content downloading request from the LCM, it confirms the LCM's ID and then downloads the content with the file format of FIG. 6 to the LCM. For the LCM to play the reached content, it follows the following steps in this order.

First, the LCM finds out the encryption algorithm from the field AIF 613 in PH 610.

Second, the fields in the secret header 620 are recovered by using the found out encryption algorithm and LCM's secret key (private key) to recover the fields in SH.

Third, the Device-ID field 621 is compared with the ID of the LCM to check if there is

correspondence between the two.

In the case of correspondence, the copy control status from the RMF data, the playback control status, and the transfer control status are identified to register them in the database(RMS-DB) which the LCM 140 has.

After the above process is performed, the digital content encryption key is extracted by using a CEK field, and the encoded digital content is interpreted by using the encryption key.

If any of the above lists is not violated, the music can be played.

If it is needed to modify the RMF624, especially the Playback Control Status (PCS), the LCM 140 has to update the data both in the file and in the RMS-DB following the controlling direction.

In the case of changing the RMF 624 of the file formats, in particular the playback control status, the LCM 140 replaces the playback control state data in two places of the database(RMS-DB) and the file format with desired data.

The procedure for the LCM 140 to download the content to its portable device 150 includes the following steps:

First, the LCM 140 requests the PD-ID and UTD to the portable device 150.

Second, the portable device 150 sends the ENC $(CK_{PD-LCM}, UTD \parallel PD-ID)$ to the LCM 140.

Third, the LCM 140 recovers the PD-ID and confirms it.

Fourth, the LCM 140 recovers the UTD and the fields in the secret header 620 and compares them with those in its RMS-DB. If UTD is correct and if any alteration of RMF is needed, the LCM updates the contents of RMF both in RMS-DB and in the file format.

Fifth, the LCM 140 updates UTD of RMS-DB with a newly generated UTD, and ENC $(CK_{PD-}$

$_{LCM}$, UTD*) is to be sent to the PD.

Sixth, where the Transfer Control Status field has the three types, "Transfer", "Transferred", and "Transfer-non", and the Transfer Control Status indicates "Transfer", ""Transfer"" is replaced with "Transferred" in the Transfer Control Status field in RMS-DB, but not in the file format. Where the Transfer Control Status field has the three types, """Transfer""", Transferred""", and """Transfer-non""".

Seventh, if the Copy Control Status (CCS) indicates "Check-in",it is replaced by "Check-out" in the Copy Control Status field both in RMS-DB and in the file format.

Eighth, if the Copy Control Status (CCS) indicates "Copy-Never", the content downloading to the portable device is denied.

If any of the above lists is not violated, the content is downloaded to the PD.

Hereinafter the process of the digital contents between the portable device 150 and the portable recording medium 160 as a content storage medium for preventing an illegal copy in downloading the digital content, which the portable device has, to the portable medium 160 is explained.

Firstly, if there is its owned ID in the portable medium 160, the portable device 150 records the digital contents which are encrypted by using the ID.

Secondly, if there is its owned ID in the portable medium 160, the portable device 140 records the digital contents which are encrypted by using randomly generated key. The randomly generated key T is encrypted by using a key, S, of the general secret key which is predetermined by the manufacturer 120 of the portable device 150.

The encrypted T is recorded on the hidden area of the PM.

Where there is its own ID in the portable medium 160, all contents within the portable medium can be played by all the portable devices, but, where there is not its own ID, all contents within the portable medium 160 can be played only by the portable devices produced by the manufacturers which adopted this system. Anyway it is certain that this system can support the portability of contents via the portable media.

Fig. 7

As shown in Fig. 7, various inputs such as originated from RedBook CD, Audio CD, Super Audio CD, DVD Disk, and analog Device are allowable to LCM optionally. An analog input to PD is also allowable. The secure import control for those several inputs to LCM or to PD is presented hereinbelow.

The audio signal inputted through the input devices is inputted to the LCM 140, and encoded according to a system supported in the present invention, and then transmitted to the portable device 150, or transmitted to the portable medium 160 to be reproduced through the portable device 150.

The kiosk 170 generates a registration request signal for selling an encoded digital content by the internet service provider 130 through the LCM 140. Therefore, the internet service provider 130 provides to the kiosk 170 the portable medium 160 having digital contents encoded by the system supported in the present invention according to the registration request signal, and the kiosk receives fees from users and transmits the digital contents stored in the portable medium 160. Kiosk 170 is a store or vending machine selling a recording medium or digital content which is reproduced in this system. Machine on Kiosk is regarded as a personal computer having an interface of the digital content portable medium 160. The recording medium interface can be used by anyone having

a supply agreement with an intellectual property right owner or the digital internet service provider.

Fig. 8

FIG. 8 is a view for showing an output source of Fig. 7 capable of being additionally connected to the embodiment of the present invention.

As shown in Fig. 8, the host device, in which the LCM module exists, has at least the following three layers (two of these exist in the LCM module).

Authenticated Input API 810 has the roles of confirming the validity of the input and extracting some required information to convert the input into a SDMI Compliant format.

With respect to the role of confirming the validity of the input, if the input data have a watermark, then this API should be able to detect it.

If the input data take an encrypted (or scrambled) form, then this API should be able to extract its encryption key and the encryption (or scrambling) algorithm.

If the input data do not take any protected form, then the API should confirm the validity of written format of the media containing the input data.

The API checks if an input device and data inputted from the input device are suitable for the system and transmits the following data to the import control layer 820.

The required data for the API to pass over to the Import Control Layer are as follows: Information of the media (source) type (*e.g.*, Audio CD, DVD Audio, Information of the originator of the input content, Information of the content (e.g., Title, if any, Player, Artist), Information of the encryption algorithm if any, Information of the encryption key if any.

The Import Control Layer 820 gets a bundle of information from the Authenticated Input API

and reconstructs the input content to meet a SDMI Compliant file format by following the rules listed below:

Copy Control Status is marked as "Copy-Never" or "Check-in/Check-out" (optionally).

Playback Control Status is marked as "Times to playback = infinite or N" (N: optional).

Transfer Control Status is marked as "Transfer-Non".

Mark the "LCM-ID" into the SOI field and Device-ID field of SH (Secret Header)

If the input content is not encrypted, a random key is generated and encrypts the input content by the random key.

If the input content takes an encrypted form by other encryption algorithm different from the PD's, then this layer trans-encrypts the content to be played in the PD.

The secret header part is encrypted by LCM's public key.

PD Interface layer 830 authenticates the connected portable device 150 by checking whether the portable device 150 has its correct ID and the secret channel key, CK_{PD-LCM}. The Kerberos Authentication Protocol may be used (refer to: A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, pp. 401-403, CRC Press, 1996).

The Import Control Layer (ILC) 860 within the portable device 150 makes a SDMI Compliant compressed digital content from the analog input by following the rules listed below:

Upon reception of each frame of the analog input, the ICL encodes the frame and by a randomly generated key. If all the frames have been encrypted, the next steps are followed.

Copy Control Status is marked as "Copy-Never" or "Check-in/Check-out" (optionally)

Playback Control Status is marked as "Times to playback = infinite or N" (N: optional).

Transfer Control Status is marked as "Transfer-Non".

The ""'PD-ID'"" is marked into the SOI field and Device-ID field of SH (Secret Header)].

The portable device encrypts the secret header part by channel key.

If the converted SDMI Compliant content from the analog input has its SOI field 622 of the Secret Header with marked "PD-ID", then the procedure of writing the content on a portable medium (PM) does not use the unique ID of the PM. This means that such content as made from an analog input to a portable device is not allowed to have the "Portability".

Hereinafter, the copy protection scheme for portable media is described.

PM may optionally support unique ID for first Generation PM. If the unique ID is not supported, the physical address of a bad sector of the portable medium is used instead. If unique ID is supported, it should be one-time writeable during the manufacturing stage only, and readable only by the portable device with a special command.

Channel key (CK) is a shared key between LCM and PD. To support portability, CK is not considered as input to function f(). If CK is included, it provides additional security to the content stored in PM. CK may take various forms depending on the application usage and right management rules.

With respect to a physical address of bad sector of a portable media, P, the usage of P prevents the playback of illegally copied content from PM to PM by simple "dead-copy".

Referring to a spared area, a special command known only to the manufacturer needs to be known to access this area.

Fig. 9

The copy protection system for the portable media is shown in FIG. 9.

First, the portable device 150 and the LCM 140 share a channel key to form a secure channel between them.

The portable device 150 receives as inputs and function processes a physical address of a bad sector of the portable medium 160, a random number, and a secret channel key which is transmitted from the LCM 140 and stored in the LCM 140. With the processed value, the portable device 150 encrypts a header of the digital contents and transmits it 160. Hash function or one way function can be used for the function process. At this time, what generates the key for encryption is the function process means 149.

Function process means 149 receives as an input the physical address of the bad sector transmitted from the portable medium 160 and receives as an input the random number through the random number generating means (RNG) 159. The random number is also transmitted and stored in a spare area of the portable medium 160.

The portable medium 160 transmits the physical address of the bad sector, stores a random number generated in the portable device 150 as an input in the spare area, and stores as sector data the encrypted header information encrypted by the processed value and the encrypted digital content inputted through the portable device 150.

It is optional to encrypt the header of the digital content by function processing after receiving all of the commonly owned key, random number, and the physical address of the bad sector or one of the commonly owned key, random number, and the physical address of the bad sector.

The digital content can be downloaded to the portable medium 160 through the portable device 150 or directly from the LCM 140.

Even if the portable medium is copied to another portable medium, the digital content in the portable medium cannot be reproduced from the portable medium. Therefore, this invention provides the effect on basically protecting illegal copy.

VI. ISSUES

Whether claim 18-40 are allowable under 35 U.S.C. §112, first paragraph.

Whether claim 1-3, 5-7, 9-23 and 25-40 are patentable under 35 U.S.C. §102(e) over Downs (US 6,574,609).

Whether claim 24 is patentable under 35 U.S.C. §103(a) over Downs (US 6,574,609) in view of Davis (US 6,041,314).

VII. GROUPING OF CLAIMS

Under §112: Claim 18 stands or falls alone. Claims 19-22 stand or fall with claim 18. Claims 23-40 stand or fall alone.

Under §102: Claims 1, 17, 18, 23, 30, 32, 37, 38 and 40 stand or fall alone. Claims 2, 3, 5-7, 9-16, 19-22, 25-29, 31, 33-36 and 39 stand or fall with the respective claims from which they depend.

Under §103: Claim 24 stands of falls alone.

VIII. ARGUMENT

Claims 18-40 were rejected under 35 U.S.C. §112, first paragraph.

On page 2 of the final Office action, the Examiner, in paragraph 1, indicates that the amendment filed 24 July 2003 is objected to under 35 U.S.C. §132 because is supposedly introduces new matter by the addition of claims 18-40.

Section (a) of §132 refers to amendments to the disclosure, not the claims. Accordingly, the objection is in error.

On pages 2-3 of the final Office action, the Examiner, in paragraphs 3 and 4, rejected claims 18-40 as failing to comply with the written description requirement. In support of the rejection, the Examiner states that the "claim(s) contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention."

The final Office action failed to identify what subject matter, *i.e.*, which feature(s), of claims 18-40 the Examiner considers to be inadequately described in the specification in such a way as to reasonably convey to one of ordinary skill in the art that the Applicant had possession of the claimed invention at the time the application was filed.

In the response to the final rejection, the rejection was challenged with respect to the subject matter of claims 18-40 which the Examiner considered to be new matter.

In the Advisory Action the Examiner provided an indication of the alleged new matter, even though the claims in which the alleged new matter appear was not identified.

The alleged new matter, as best can be understood from the Advisory Action, is as follows:

(a) terminal receiving and function-processing a physical address of a bad sector of the storage medium, a random number generated and stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain a processed value and said terminal encrypting a header of the digital content with the processed value,

(b) portable terminal supplier embedding the manufacturer key information in said portable terminal,

(c) certificate authority and content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said encrypted digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said encrypted digital content,

(d) personal computer having public key information of said certificate authority, said personal computer and said content supplier sharing a second secret channel, said personal computer verifying said first key information,

(e) supplier by using said public key information of said certificate authority and receiving the second key information through said second secret channel,

(f) said personal computer receiving said encrypted digital content through said second secret channel,

(g) portable terminal transferring the embedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said portable terminal and said personal computer sharing a third secret channel for transferring said encrypted digital content between said portable terminal and said personal computer,

(h) supplier to form said first secret channel,

(i) the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key,

(j) personal computer to form said second secret channel and the second key

information is encoded by said second channel key and then transferred to said personal computer,

(k)   certificate authority generating first key information for giving authorization to supply said digital content, said certificate authority generating a token to make an information table, token information encrypted by said manufacturer key,

(l)   updating reproduction data whenever any content downloading or uploading session between said first content output means and said second content output means occurs.

It is not entirely clear what the Examiner is stating, and the following arguments are based upon further analysis of the Examiner's comments.

With respect to the first feature (a) above, claim 18 calls for *said terminal receiving and function-processing a physical address of a bad sector of the storage medium, a random number generated and stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain a processed value, said terminal encrypting a header of the digital content with the processed value.*

Such a terminal is shown in Fig. 1 as element 150. Looking to the specification, we find it disclosed that "The portable device 150 receives as inputs and function processes a physical address of a bad sector of the portable medium 160, a random number, and a secret channel key which is transmitted from the LCM 140 and stored in the LCM 140. With the processed value, the portable device 150 encrypts a header of the digital contents and transmits it 160." The foregoing corresponds to the original disclosure, which states: "portable terminal 50 contains a random number generation unit (RNG) for randomly generating a number, and a function process unit (F) for function-processing various inputs and generating predetermined values which only the content storage unit

60 can have. At this time, values inputted to the function process unit (F) are a random number, a channel key, and a bad sector address and an inherent number which the content storage unit 60 inherently has. Further, another encryption of an encoded digital content reproduction data is performed by using function values generated in the function process unit (F);" and also states "The system includes a portable terminal processing the random number stored in spare area of the digital content storage medium such as physical address of the bad sector of the digital content storage medium and transmitting the encrypted header of the digital content by using the processed value of the random number, and a digital content storage medium reading and transmitting the physical address by using the portable terminal and storing the number as a key value randomly generated by the portable terminal, and storing the encrypted header information encrypted by the resultant value and the encrypted digital content as sector data."

Also, note that claim 17 contains similar language to claim 18, in that claim 17 calls for "a terminal receiving a physical address of a bad sector of a storage medium, said terminal generating a random number and storing said random number in a spare area of said storage medium, said terminal having a secret channel key, said terminal function-processing said physical address, said random number and said secret channel key to obtain a processed value, said terminal encrypting a header of the digital content by the processed value."

Claim 17 was not rejected on the grounds of new matter.

Accordingly, there is clear support for the feature (a) mentioned by the Examiner.

With respect to the feature (b) mentioned by the Examiner, there is no claimed phrase "portable terminal supplier" in any of claims 18-40. Claim 18 calls for, *said terminal supplier*

embedding the manufacturer key information in said terminal. Such a terminal supplier is shown in Fig: 1 as element 120. The specification states: "When the manufacturer 120 requests its registration to CA 110, CA 110 certifies it and then generates a manufacturer key, MK_{PD}, and make its certificate data, $Cert_{CA}(MK_{PD})$, to deliver them to the manufacturer 120. At the same time CA 110 generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for an ISP-registration. Once after the manufacturer 120 gets the data, $\{MK_{PD}, Cert_{CA}(MK_{PD})\}$, the manufacturer 120 can manufacture the portable devices by imbedding those secret data within a temper resistant area of the portable devices."

Additionally, claim 1, not rejected on new matter, does call the terminal supplier a *portable terminal supplier* and includes the feature of *said portable terminal supplier imbedding the manufacturer key information in said portable terminal.* Embedding and imbedding are alternative spellings and have the same meaning.

Accordingly, the feature (b) mentioned by the Examiner has clear support in the specification and was not rejected with respect to claim 1. Thus it is not clear why the Examiner deems this feature to be new matter.

Regarding the feature (c) mentioned by the Examiner, claim 18 calls for *a content supplier sending a second registration request signal to the certificate authority, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said digital content from said*

second key information.

Claim 1, not rejected on the ground of new matter, calls for "a content supplier transmitting a second registration request signal to the certificate authority, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said encrypted digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said encrypted digital content."

Accordingly, it is not clear why the feature (c) is being rejected seeing that nearly the same terminology is used in claim 1.

Additionally, the specification states: "A content supply unit 30 outputs the second registration request signal to the authorization recognition unit, stores the first authentication qualification key, the first authentication qualification key data, and the second table, and generates a second authentication qualification key and a second authentication qualification key data in response to a third registration request signal inputted from external.

A PC 40 as a first content output unit outputs the third registration request signal to the content supply unit 30 in order to receive the digital contents and output the received digital contents, stores the second authentication qualification key and the second authentication qualification key data such as Public key and Public Key information inputted from the content supply unit, outputs the manufacturer key data inputted from external to the content supply unit, encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data."

Regarding the feature (d), mentioned by the Examiner, claim 18 calls for *a personal*

computer sending a third registration request signal to the content supplier for obtaining said

second key information, said personal computer having public key information of said certificate

authority, said personal computer and said content supplier sharing a second secret channel, said

personal computer verifying said first key information .

Claim 1, not rejected on the grounds of new matter, calls for "a personal computer outputting

a third registration request signal to the content supplier for obtaining said second key information,

said personal computer having public key information of said certificate authority, said personal

computer and said content supplier sharing a second secret channel, said personal computer verifying

said first key information."

Accordingly, it is not clear why the feature (d) of claim 18 is being rejected seeing that nearly

the same terminology is used in claim 1.

Regarding the features (e) and (f), mentioned by the Examiner, claim 18 calls for *said*

personal computer verifying said first key information inputted from the content supplier by using

said public key information of said certificate authority and receiving the second key information

through said second secret channel, said personal computer receiving said digital content through

said second secret channel.

Claim 1, not rejected on the grounds of new matter, calls for "said personal computer

verifying said first key information inputted from the content supplier by using said public key

information of said certificate authority and receiving the second key information through said

second secret channel, said personal computer receiving said encrypted digital content through said

second secret channel."

The terminology of these features of claims 1 and 18 being the same, it is not clear why the features (e) and (f) are being rejected.

With respect to the feature (g), mentioned by the Examiner, it is not clear whhere, in claims 18-40, the feature is claimed. Claim 18 includes language similar to the feature (g), wherein claim 18 calls for *said terminal transferring the embedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said terminal and said personal computer sharing a third secret channel for transferring said digital content between said terminal and said personal computer.*

Looking at feature (g), however, the Examiner refers to "portable terminal transferring the embedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said portable terminal and said personal computer sharing a third secret channel for transferring said encrypted digital content between said portable terminal and said personal computer."

Claim 1 calls for "said portable terminal manufactured by said portable terminal supplier for reproducing said digital content, said portable terminal transferring the imbedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said portable terminal and said personal computer sharing a third secret channel for transferring said encrypted digital content between said portable terminal and said personal computer."

Accordingly, it appears that the language used by the Examiner is found in claim 1, not claims 18-40. Claim 1 has not been rejected on the grounds of new matter, however.

·Regarding feature (h), mentioned by the Examiner, it appears to come from language set forth in claim 19, i.e., *wherein the certificate authority generates a first channel key shared with the content supplier to form said first secret channel.*

Claim 2 calls for "wherein the certificate authority generates a first channel key shared with the content supplier to form said first secret channel."

Claim 2 has not been rejected on the grounds of new matter, thus it is not clear why feature (h) has been rejected with respect to claims 18-40.

Regarding feature (i), mentioned by the Examiner, claim 19 calls for *the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key.*

Claim 2, not rejected on the grounds of new matter, calls for an identical feature by claiming "the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key."

Accordingly, it is not clear why the Examiner has rejected feature (i) of claim 19, when the same feature is found in claim 2.

Regarding feature (j), mentioned by the Examiner, claim 19 calls for *the content supplier generates a second channel key shared with the personal computer to form said second secret channel, and the second key information is encoded by the second channel key, and then transferred to said personal computer.*

Claim 3, not rejected on the grounds of new matter, calls for "wherein the content supplier generates a second channel key shared with the personal computer to form said second secret channel, and the second key information is encoded by said second channel key, and then transferred to said personal computer."

Accordingly, it is not clear why the Examiner has rejected feature (j) of claim 19, when the same feature is found in claim 3.

Regarding feature (k), mentioned by the Examiner, the feature does not appear to be in any of claims 18-40. The feature can be found in claim 5, however claim 5 was not rejected on the grounds of new matter.

Note that the specification states, "In Fig. 2, when a manufacturer request its registration to CA, CA certifies it and then generates a manufacturer key, $MK_{PD,}$ and make its certificate data, $CertCA(ID_{MK})$, to deliver them to the manufacturer. At the same time CA generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for the other ISP-registration. Once after a manufacturer got the data, $\{MK_{PD}, Cert_{CA}(IDMK)\}$, he/she can manufactures PDs by imbedding those secrete data within a temper resistant area of Pds."

Regarding feature (l), mentioned by the Examiner, claim 20 calls for *updating the reproduction data whenever any content downloading or uploading session between said terminal and said personal computer occurs.*

Claim 13, not rejected on the grounds of new matter, calls for "updating the reproduction data whenever any content downloading or uploading session between said first content output means and

said second content output means occurs."

In claim 13, the first content output means refers to the portable terminal and the second content output means refers to the personal computer. Accordingly, the language (feature (l)) of claim 20 is similar to that of claim 13.

Therefore, since claim 13 has not been rejected on the basis of new matter, then claim 20 should not be rejected.

Accordingly, it has been shown that the language referred to by the Examiner has support in either the specification or in claims 1-7, not rejected on the basis of new matter. Thus the rejection should not be sustained.

There has been no indication of what the alleged new matter is in claims 23-40. Accordingly, absent a *prima facie* showing of new matter, claims 23-40 are deemed to be allowable under 35 U.S.C. §112, first paragraph. Thus the rejection should not be sustained.

Claims 1-3, 5-7, 9-23 and 25-40 were rejected under 35 U.S.C. §102(e) as being anticipated by Downs.

Claim 1 calls for, in part, *a certificate authority for generating manufacturer key information and generating first key information for giving an authorization to supply said encrypted digital content* . The *manufacturer key information* is provided to *a portable terminal supplier supplying a portable terminal*. A portable terminal is, for example, an end-user device similar in many ways

to the End-User Device 109 disclosed in Down's.

With respect to the claimed *certificate authority for generating manufacturer key information*, the Examiner refers us to Downs' "Clearinghouse," which is described as having the function of providing licensing authorization by enabling intermediate or End-User(s) to unlock content after verification of a successful completion of a licensing transaction.

Down's discloses, however, that license control requires that a Content Provider 101, a Electronic Digital Content Store 103, and a Clearinghouse 105 have bona-fide cryptographic digital certificates from reputable **Certificate Authorities** that are used to authenticate those components. The End-User Device 109 are not required to have digital certificates.

Accordingly, Downs clearly differentiates well known **Certificate Authorities** from Downs' Clearinghouse 105. Therefore, under §102, Downs' Clearinghouse is not equivalent to a well known **Certificate Authority**, and it is clear error to suggest that Downs' Clearinghouse corresponds to the applicant's claimed *certificate authority*.

"There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ2d 1001, 18 USPQ2d 1896 (Fed. Cir. 1991).

Note that in order for an anticipation rejection to be proper, the anticipating reference must disclose exactly what is claimed. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Therefore, since Downs' Clearinghouse does not correspond to the claimed *certificate authority*, the rejection is deemed to be in error for failing to disclose exactly what is claimed, and the §102 rejection of claims 1-3, 5-7, 9-16 and 18-22, each of which include the feature of a *certificate authority*, should not be sustained.

Additionally, according to the Applicant's disclosed invention, the Manufacturer Key, MK_{PD}, which is a pre-set manufacturer key in a tamper resistant area within the PD (SDMI (Secure Digital Music Initiative) Compliant Portable Device), is to be used for the secure registration of a PD to LCM (Licensed SDMI (Secure Digital Music Initiative) Compliant Module). Prior to manufacturing PD, the manufacturers should register to the CA **(Certificate Authority)** to get their manufacturer key, MK_{PD}, and its certificate, $Cert_{CA}(ID_{MK})$, and then produce the SDMI Compliant Portable Devices by using them. Where such registered manufacturer keys are securely stored in the CA's DB (database) and only the CA maintains the information. The manufacturer should keep their manufacturer-key and its certificate safe, maintain them securely, and embed them in a tamper resistant area of the manufactured PDs during manufacture of the PDs.

According to Downs' disclosure the "End-User Device 109 are not required to have digital certificates." Additionally, Downs discloses the End-User Device(s) 169 do not need to include certificates in their SC (Secure Container) because many End-User(s) do not bother to acquire a certificate or have certificates issued by non bona-fide **Certification Authorities**. In the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 105 has the option of issuing certificates to the Electronic Digital Content Store(s) 103. This allows the End-User Device(s) 109 to independently verify that the Electronic Digital Content Store(s) 103 have been

authorized by the Secure Digital Content Electronic Distribution System 100.

In Downs' system the "architecture requires that the Electronic Digital Content Store(s) 103 assigns a unique application ID to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application license verification." And that Downs' license control "requires that the Content Provider(s) 101, the Electronic Digital Content Store(s) 103, and the Clearinghouse(s) 105 have bona-fide cryptographic digital certificates from reputable Certificate Authorities that are used to authenticate those components. The End-User Device(s) 109 are not required to have digital certificates."

Accordingly, the *portable terminal* in Downs (End-User Device 109) does not receive and store in a tamper resistant area, *manufacturer key information* provided by a *certificate authority* as required by the instant claims, but instead stores a **unique application ID** to a downloaded Player Application 195, the unique application ID being **assigned by an Electronic Digital Content Store 103** (not a Certificate Authority nor a Clearinghouse).

Therefore, Downs fails to exactly what is claimed, thus the § 102 rejection of claims 1-3, 5-7, 9-16, 18-23 and 25-40, each of which include the feature of a *manufacturer key* or *manufacturer key information*, should not be sustained.

Claim 1 also calls for *a portable terminal supplier supplying a portable terminal, said portable terminal supplier outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said portable terminal supplier imbedding the manufacturer key information in said portable terminal.*

The Examiner fails to identify where Downs discloses such a *portable terminal supplier supplying a portable terminal.* Note, *Ex parte Levy,* 17 USPQ2d 1461, 1462 (1990) states:

> "it is incumbent upon the examiner to identify wherein each and every facet of the claimed invention is disclosed in the applied reference."

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly what is claimed. Accordingly, the §102 rejection of claims 1-3, and 18-22, each of which contains the feature of a *terminal supplier,* is not proper and should not be sustained.

The foregoing arguments have shown that each of claims 1-3, 5-7, 9-6, 18-23 and 25-40 are not anticipated by Downs. Accordingly, the rejection is deemed to be in error and should not be sustained.

Additionally, claim 17 is not anticipated by Downs because Downs fails to disclose *a terminal receiving a physical address of a bad sector of a storage medium.* The Examiner fails to identify where Downs discloses such *a terminal receiving a physical address of a bad sector of a storage medium.* Note, *Ex parte Levy,* supra.

Further, There are no **headers** disclosed in Downs. Claim 17 calls for *said terminal encrypting a header of the digital content by the processed value.*

Accordingly, the rejection is deemed to be in error and should not be sustained.

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly what is claimed. Claims 18 and 40 also refer to the *bad sector* and are deemed to not be anticipated

by Downs. Claim 18 also calls for *said terminal encrypting a header of the digital content with the processed value.* Accordingly, the §102 rejection of claims 17, 18 and 40 is not proper and should not be sustained.

Regarding claim 23, it is required that a *server* comprise *a first cryptosystem verifying public key information of a content provider by using public key information embedded in said server to check whether said content provider has an authorization to supply said digital content,* and *a second cryptosystem encrypting and transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider.*

Note, *Ex parte Levy*, supra.

The Examiner fails to identify where each feature of claim 23 is found in Downs. It is noted that Downs fails to disclose, for example, *first* and *second cryptosystems, public key information embedded in said server* and *manufacturer key information.*

Note for example, that since Downs fails to disclose such *manufacturer key information* the cannot possibly be a second cryptosystem encrypting and transferring manufacturer key information embedded in a terminal from the terminal to a content provider to be verified by the content provider, such that the server will establish a secure channel to the terminal after the validation of the manufacturer key information disclosed in Downs. Also, the Examiner fails to identify where Downs discloses *transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider.*

Accordingly, the rejection is deemed to be in error and should not be sustained.

Regarding claim 30, it is required that the *digital content* have a first file format comprising *a plain header comprising a title identifier, a content description field, and an algorithm identifying field from which said server finds out an encryption algorithm and a secret key of said server*; and *a secret header comprising a device identifier to be compared with an identifier of said server, an indicator of a source origination of said digital content, a right management field including data to be registered to said right management system, and a content encryption key for recovering said digital content encrypted by said content encryption key.*

There are no **headers** disclosed in Downs. See also claims 37 and 38. Accordingly, the rejection is deemed to be in error and should not be sustained.

Claim 32 calls for *manufacturer key information embedded in said terminal*. Downs is silent in this regard. Accordingly, the rejection is deemed to be in error and should not be sustained.

Claim 24 was rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Downs in view of Davis.

Claim 24 depends from claim 23. Claim 23 calls for *a second cryptosystem encrypting and transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider, said server establishing a third secure channel to said terminal after the validation of the manufacturer key information.*

As noted above with respect to the §102 rejection, Downs fails to disclose *manufacturer key information*.

Accordingly, since Downs fails to disclose such *manufacturer key information* the cannot possibly be a second cryptosystem encrypting and transferring manufacturer key information embedded in a terminal from the terminal to a content provider to be verified by the content provider, such that the server will establish a secure channel to the terminal after the validation of the manufacturer key information disclosed in Downs. Examiner fails to identify where Downs discloses *transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider*. Note, *Ex parte Levy*, supra.

Davis was not applied as a teaching of *manufacturer key information* nor as a teaching of *transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider*.

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly what is claimed. Accordingly, the §102 rejection of claim 23 is not proper and, since claim 24 depends from claim 23, the §103 rejection is not proper and should not be sustained.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.

Washington, D.C. 20005
(202) 408-9040

Folio: P55690
Date: 7/26/04
I.D.: REB/MDP

IX. APPENDIX

CLAIMS UNDER APPEAL

Claims 1-3, 5-7 and 9-40 are pending

1   1.   A system for preventing an illegal copy of digital content, said system receiving and

2   decrypting encrypted digital content and reproducing the digital content, comprising:

3   a certificate authority for generating manufacturer key information and generating first key

4   information for giving an authorization to supply said encrypted digital content;

5   a portable terminal supplier supplying a portable terminal, said portable terminal supplier

6   outputting a first registration request signal to said certificate authority and receiving the

7   manufacturer key information generated by said certificate authority in accordance with the first

8   registration request signal, said portable terminal supplier imbedding the manufacturer key

9   information in said portable terminal;

10   a content supplier transmitting a second registration request signal to the certificate authority,

11   said certificate authority and said content supplier sharing a first secret channel, said content supplier

12   receiving and storing said first key information from the certificate authority through said first secret

13   channel for supplying said encrypted digital content, said content supplier generating and outputting

14   second key information for giving an authorization to receive and reproduce said encrypted digital

15   content;

16   a personal computer outputting a third registration request signal to the content supplier for

17   obtaining said second key information, said personal computer having public key information of said

18   certificate authority, said personal computer and said content supplier sharing a second secret

19 channel, said personal computer verifying said first key information inputted from the content

20 supplier by using said public key information of said certificate authority and receiving the second

21 key information through said second secret channel, said personal computer receiving said encrypted

22 digital content through said second secret channel; and

23 said portable terminal manufactured by said portable terminal supplier for reproducing said

24 digital content, said portable terminal transferring the imbedded manufacturer key information to

25 said content supplier through said personal computer to be verified by said content supplier, said

26 portable terminal and said personal computer sharing a third secret channel for transferring said

27 encrypted digital content between said portable terminal and said personal computer.

1   2.   The system as claimed in claim 1, wherein the certificate authority generates a first

2 channel key shared with the content supplier to form said first secret channel, the first key

3 information is encoded by said first channel key and then transferred to said content supplier, and

4 said content supplier decodes the encoded first key information by said first channel key.

1   3.   The system as claimed in claim 1, wherein the content supplier generates a second

2 channel key shared with the personal computer to form said second secret channel, and the second

3 key information is encoded by said second channel key, and then transferred to said personal

4 computer.

1   5.   A system for preventing an illegal copy of digital content, comprising:

2   a certificate authority for generating manufacturer key information comprising a

3 manufacturer key and a manufacturer key data in response to a first registration request signal

4 inputted from an external source, generating first key information for giving an authorization to

5 supply said digital content, said certificate authority generating a token to make an information table,

6 said information table comprising a first table containing the manufacturer key data, the

7 manufacturer key, and an identifier corresponding to the manufacturer key, and a second table

8 containing said identifier, token information encrypted by said manufacturer key, and said token;

9 a content supplier transmitting a second registration request signal to the certificate authority

10 for supplying said digital content, said certificate authority and said content supplier sharing a first

11 secret channel, said content supplier receiving and storing said first key information and said second

12 table from the certificate authority through said first secret channel, said content supplier generating

13 second key information;

14 first content output means for outputting the digital content, said first content output means

15 sending a third registration request signal to the content supplier for downloading said digital content

16 from said content supplier, said first content output means having public key information of said

17 certificate authority, said first content output means and said content supplier sharing a second secret

18 channel, said first content output means verifying said first key information inputted from the content

19 supplier by using said public key information of said certificate authority and receiving the second

20 key information through said second secret channel, said first content output means extracting the

21 manufacturer key information from said second table, and encoding and outputting the manufacturer

22 key information; and

23 said second content output means for recording and reproducing said digital content, said

24 second content output means storing the manufacturer key information, said second output means

25 transferring said manufacturer key information to said content supplier through said first content

26 output means to be verified by said content supplier, said second content output means receiving said

27 manufacturer key information of said second table from said first content output means to decide if

28 the manufacturer key is authenticated, said second content output means and said first content output

29 means sharing a third secret channel for transferring said digital content between said second content

30 output means and said first content output means.

1   6.   The system claimed in claim 5, wherein a content storage means is further included in

2 at least one of said second content output means and said first content output means, and said content

3 storage means stores said digital content.

1   7.   The system claimed in claim 5, wherein the certificate authority generates a first channel

2 key shared with the content supplier to form said first secret channel, the first key information is

3 encoded by said first channel key and then transferred to said content supplier, and said content

4 supplier decodes the encoded first key information by said first channel key.

1   9.   The system claimed in claim 5, wherein the content supplier generates a second channel

2 key shared with the first content output means to form said second secret channel, and the second

3 key information is encoded by the second channel key, and then transferred to said first content

4 output means.

1   10.   The system claimed in claim 5, wherein the token is randomly generated by the

2   certificate authority.

1   11.   The system claimed in claim 7, wherein the first content output means generates a third

2   channel key shared with the second content output means to form said third secret channel, and the

3   first content output means encodes the third channel key with said token inputted from the content

4   supplier and transmits the third channel key to the second content output means.

1   12.   The system claimed in claim 11, the second content output means decodes the encoded

2   token transmitted from the first content output means by using the stored manufacturer key, decodes

3   and stores the third channel key by using said token.

1   13.   The system claimed in claim 11, further comprised of:

2   said first content output means including a database which has reproduction data of the

3   digital content downloaded from the content supplier, said first content output means encoding the

4   database by using the third channel key for storage, interpreting the reproduction data of the digital

5   content by using the third channel key to thereby judge if an illegal copy of the digital content is

6   performed; and

7   said second content output means receiving said reproduction data from said first content

8   output means, updating the reproduction data whenever any content downloading or uploading

9   session between said first content output means and said second content output means occurs, and

10   transmitting the updated reproduction data of the digital content to the first content output means.

1 14. The system claimed in claim 13, wherein the database is separated with an identifier

2 data area of the digital content, an updated token data area, a data area for a present state of the

3 digital content, and a reproduction control data area, and has the corresponding data.

1 15. The system claimed in claim 14, wherein the data area for the present state of the

2 digital content comprises:

3 first data indicating that the digital content is downloaded in a copy form from the first

4 content output means to the second content output means;

5 second data indicating that the digital content is downloaded in a transmission form from the

6 first content output means to the second content output means; and

7 third data indicating that the digital content is downloaded and uploaded between the first

8 content output means and the second content output means.

1 16. The system claimed in claim 14, wherein the reproduction control data area of the

2 digital content includes:

3 fourth data for reproduction times of the digital content;

4 fifth data for a reproduction expiration period of the digital content; and

5 sixth data for an amnesty period of the digital content.

1 17. A system for protecting a illegal copy, comprising:

2 a terminal receiving a physical address of a bad sector of a storage medium, said terminal

3 generating a random number and storing said random number in a spare area of said storage medium,

4   said terminal having a secret channel key, said terminal function-processing said physical address,

5   said random number and said secret channel key to obtain a processed value, said terminal

6   encrypting a header of the digital content by the processed value; and

7   said storage medium transmitting said physical address of the bad sector, storing said random

8   number as a key value generated from said terminal, storing as a sector data the encrypted digital

9   content and the header of the digital content encrypted by using the processed value.

1   18.   A system for protecting an illegal copy of digital content, comprising:

2   a certificate authority for generating manufacturer key information and generating first key

3   information for giving an authorization to supply said digital content;

4   a terminal supplier supplying a terminal, said terminal supplier outputting a first registration

5   request signal to said certificate authority and receiving the manufacturer key information generated

6   by said certificate authority in accordance with the first registration request signal, said terminal

7   supplier embedding the manufacturer key information in said terminal;

8   a content supplier sending a second registration request signal to the certificate authority, said

9   certificate authority and said content supplier sharing a first secret channel, said content supplier

10   receiving and storing said first key information from the certificate authority through said first secret

11   channel for supplying said digital content, said content supplier generating and outputting second

12   key information for giving an authorization to receive and reproduce said digital content from said

13   second key information;

14   a personal computer sending a third registration request signal to the content supplier for

15   obtaining said second key information, said personal computer having public key information of said

16 certificate authority, said personal computer and said content supplier sharing a second secret

17 channel, said personal computer verifying said first key information inputted from the content

18 supplier by using said public key information of said certificate authority and receiving the second

19 key information through said second secret channel, said personal computer receiving said digital

20 content through said second secret channel;

21 said terminal manufactured by said terminal supplier for reproducing said digital content and

22 reading a storage medium, said terminal transferring the embedded manufacturer key information

23 to said content supplier through said personal computer to be verified by said content supplier, said

24 terminal and said personal computer sharing a third secret channel for transferring said digital

25 content between said terminal and said personal computer, said terminal receiving and function-

26 processing a physical address of a bad sector of the storage medium, a random number generated and

27 stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain

28 a processed value, said terminal encrypting a header of the digital content with the processed value;

29 and

30 said storage medium transmitting said physical address of the bad sector, storing said random

31 number as a key value generated from said terminal, storing as a sector data the encrypted header of

32 the digital content and encrypted header information encrypted by using the result of function

33 processing.

1 19. The system claimed in claim 18, wherein the certificate authority generates a first

2 channel key shared with the content supplier to form said first secret channel, the first key

3 information is encoded by said first channel key and then transferred to said content supplier, and

4   said content supplier decodes the encoded first key information by said first channel key, the content

5   supplier generates a second channel key shared with the personal computer to form said second

6   secret channel, and the second key information is encoded by the second channel key, and then

7   transferred to said personal computer, and the personal computer generates a third channel key

8   shared with the terminal to form said third secret channel, and the personal computer encodes the

9   third channel key with said token inputted from the content supplier and transmits the third channel

10   key to the terminal.

1   20.   The system claimed in claim 19, further comprised of:

2   said personal computer having a database which comprises reproduction data of the digital

3   content downloaded from the content supplier, the database encoded by using the third channel key,

4   said personal computer interpreting the digital content by using the third channel key to decide if an

5   illegal copy of the digital content is performed; and

6   said terminal receiving said reproduction data from said personal computer, updating the

7   reproduction data whenever any content downloading or uploading session between said terminal

8   and said personal computer occurs, and transmitting the updated reproduction data to the personal

9   computer.

1   21.   The system claimed in claim 20, wherein the database is separated with an identifier

2   data area of the digital content, an updated token data area, and a data area for a present state of the

3   digital content, and a reproduction control data area.

1   22.   The system claimed in claim 21, wherein the data area for the present state of the

2   digital content includes first data indicating that the digital content is downloaded in a copy form

3   from the personal computer to the terminal. second data indicating that the digital content is

4   downloaded in a transmission form from the personal computer to the terminal, and third data

5   indicating that the digital content is downloaded and uploaded between the personal computer and

6   the terminal, and the reproduction control data area of the digital content includes fourth data for

7   reproduction times of the digital content, fifth data for a reproduction expiration period of the digital

8   content; and sixth data for an amnesty period of the digital content.

1   23.   A server for preventing an unauthorized copy of digital content, said server comprising:

2   a first cryptosystem verifying public key information of a content provider by using public

3   key information embedded in said server to check whether said content provider has an authorization

4   to supply said digital content, said server establishing a second secure channel to said content

5   provider to download said digital content from said content provider;

6   a second cryptosystem encrypting and transferring manufacturer key information embedded

7   in a terminal linked to said server from said terminal to said content provider to be verified by said

8   content provider, said server establishing a third secure channel to said terminal after the validation

9   of the manufacturer key information, said server transferring a token of said content provider to said

10   terminal through said second secure channel and said third secure channel; and

11   a secure check-in and check-out system for checking a validation of said digital content, said

12   secure check-in and check-out system comprising a right management system having a right

13   management database, wherein information of said digital content corresponding to said right

14 management database is registered to said right management system, said right management database

15 is updated whenever said digital content is downloaded or uploaded between said server and said

16 terminal to check if an unauthorized copy of said digital content is performed.

1   24.   The server of claim 23, wherein said second secure channel is established by executing

2   a handshaking protocol to get an ephemeral shared key by utilizing Elliptic curve based key

3   exchanging protocol.

1   25.   The server of claim 23, wherein said third secure channel is established by a third

2   secret channel key generated in one of said server and said terminal.

1   26.   The server of claim 25, wherein said right management database comprises

2   reproduction data of said digital content, said server encodes said reproduction data by using said

3   third secure channel key, and said server checks said reproduction data by using said third secure

4   channel key.

1   27.   The server of claim 25, wherein said right management database comprises an

2   identifier data area of the digital content, an updated token data area, a data area for a present state

3   of the digital content, and a reproduction control data area.

1   28.   The server of claim 27, wherein the data area for the present state of the digital content

2   comprises:

3   first data indicating that the digital content is downloaded in a copy form from said server

4   to said terminal;

5   second data indicating that the digital content is downloaded in a transmission form from said

6   server to said terminal; and

7   third data indicating that the digital content is downloaded and uploaded between said server

8   and said terminal.

1   29.   The server of claim 27, wherein the reproduction control data area of the digital

2   content comprises:

3   fourth data indicating reproduction times of the digital content;

4   fifth data indicating a reproduction expiration period of the digital content; and

5   sixth data indicating an amnesty period of the digital content.

1   30.   The server of claim 27, wherein said digital content has a first file format comprises:

2   a plain header comprising a title identifier, a content description field, and an algorithm

3   identifying field from which said server finds out an encryption algorithm and a secret key of said

4   server;

5   a secret header comprising a device identifier to be compared with an identifier of said server,

6   an indicator of a source origination of said digital content, a right management field including data

7   to be registered to said right management system, and a content encryption key for recovering said

8   digital content encrypted by said content encryption key; and

9   a file body comprising said digital content encrypted by using said content encryption key.

1   31.   The server of claim 30, further comprising:

2   an applied program interface confirming a validity of an input and extracting first information

3   from said input;

4   an import control layer receiving said first information from said applied program interface,

5   said import control layer reconstructing said first information into said first file format; and

6   a terminal interface authenticating said terminal by checking whether said terminal has a

7   correct identifier and said third secret channel key.

1   32.   A terminal, comprising:

2   manufacturer key information embedded in said terminal; and

3   a symmetric key cryptosystem preventing an unauthorized copy of digital content by

4   responding to reception of said manufacturer key information by a server by establishing a secure

5   registration of said terminal with said server, with said terminal establishing a third secure channel

6   to said server and said terminal receiving a token from said server through said third secure channel

7   to reproduce said digital content provided by said server.

1   33.   The terminal of claim 32, further comprising:

2   a public key cryptosystem, wherein said terminal verifies public key information of said

3   server by using public key information embedded in said terminal to check whether said server has

4   an authorization to download said digital content to said terminal.

34. The terminal of claim 32, wherein said terminal generates update token data whenever said digital content is downloaded or uploaded between said terminal and said server to check if an unauthorized copy of said digital content is performed.

35. The terminal of claim 34, wherein said third secure channel is established by a third secret channel key.

36. The terminal of claim 35, wherein said update token data are encoded and decoded by said third secret channel key.

37. The terminal of claim 32, wherein said digital content has a first file format comprising:

a plain header comprising a title identifier, a content description field, and an algorithm identifying field;

a secret header comprising a device identifier, an indicator of a source origination of said digital content, a right management field, and a content encryption key for recovering said digital content encrypted by said content encryption key; and

a file body comprising said digital content encrypted by said content encryption key.

38. The terminal of claim 37, wherein said terminal is able to write said digital content encrypted by said content encryption key on a storage medium, recover said secret header, and reencrypt said digital content by using an unique identifier in said storage medium, and, if said

4 storage medium does not have said unique identifier in said storage medium, said terminal is able

5 to write said digital content encrypted by said content encryption key on said storage medium,

6 recover said secret header, reencrypt said digital content by using a randomly generated key, and

7 encrypt and write said randomly generated key on a hidden area of said storage medium by using a

8 common secret key embedded in said terminal.

1   39.   The terminal of claim 37, wherein said terminal has an import control layer to convert

2 an analog input to said digital content having said first file format.

1   40.   The terminal of claim 38, wherein said unique identifier is a physical address of a bad

2 sector of said storage medium, said terminal has a random number generator to generate a random

3 number and stores said random number in a spare area of said storage medium, and said terminal has

4 a function-processor function-processing said physical address, said random number and said third

5 secure channel key to obtain a processed value, and said terminal encrypts said digital content with

6 the processed value.